PAT-NO: JP410013945A

DOCUMENT-IDENTIFIER: JP 10013945 A

TITLE: ROAMING SYSTEM

PUBN-DATE: January 16, 1998

INVENTOR-INFORMATION:
NAME
TOMOIKE, HIROMOTO

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NEC CORP	N/A

APPL-NO: JP08161647

APPL-DATE: June 21, 1996

INT-CL (IPC): H04Q007/38, H04L009/30 , H04L009/32

ABSTRACT:

PROBLEM TO BE SOLVED: To provide a roaming system which can perform roaming processing, without notifying proper information about a subscriber number and a terminal of an authentication key, etc., to a roaming bound network.

SOLUTION: A roaming terminal 10 encrypts a subscriber number MSN with a public key Kpa of a home network and sends it to a home network 30 through a roaming bound network 20. The network 30 decodes cipher with a secret key Ksa, acquires the MSN and an authentication key Sa, which is temporarily generated with a public key Kp1 of a terminal which corresponds to the MSN. When the key Sa is notified to the network 20 and an encrypted authentication key is notified to the terminal 10, the network 30 authenticates a terminal

by using a random number which is generated and using these authentication keys. When **authentication** is completed, the network 20 acquires a **roaming number** and notifies it to the terminal 10 and the network 30. The terminal 10, the networks 20 and 30 separately store the **roaming number and the authentication** key.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－13945

(43)公開日　平成10年(1998)１月16日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｑ	7/38			Ｈ０４Ｂ	7/26	１０９Ｈ
Ｈ０４Ｌ	9/30			Ｈ０４Ｌ	9/00	６６３Ｚ
	9/32					６７３Ｂ
						６７３Ｃ

審査請求　有　　請求項の数９　ＯＬ　（全９頁）

(21)出願番号　特願平8－161647

(22)出願日　平成８年(1996)６月21日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　友池　裕元
東京都港区芝五丁目７番１号　日本電気株式会社内

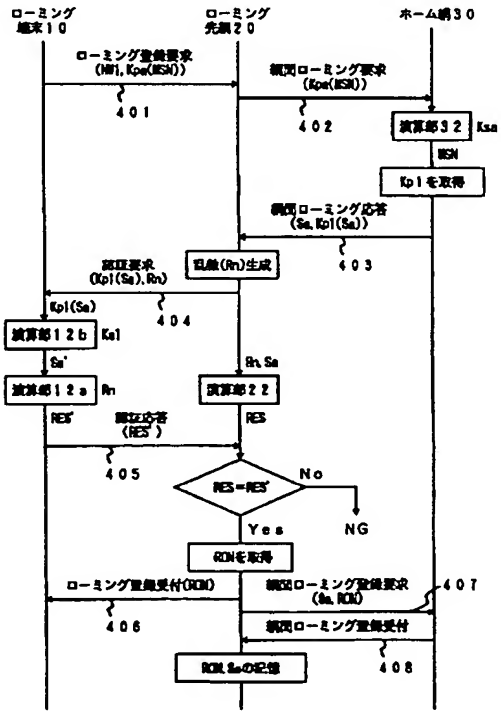
(74)代理人　弁理士　後藤　洋介　（外２名）

(54)【発明の名称】　ローミング方式

(57)【要約】

【課題】　加入者番号や、認証鍵等の端末に関する固有情報をローミング先網に通知することなく、ローミング処理を行うことできるローミング方式を提供する。

【解決手段】　ローミング端末１０は、加入者番号ＭＳＮをホーム網の公開鍵Ｋpaで暗号化し、ローミング先網２０を介してホーム網３０へ送信する。ホーム網３０は秘密鍵Ｋsaで暗号を解読してＭＳＮを得、一時的に生成した認証鍵Ｓa をＭＳＮに対応する端末の公開鍵Ｋp1で暗号化する。認証鍵Ｓa がローミング先網に通知され、暗号化された認証鍵がローミング端末に通知されると、ローミング先網が発生した乱数とこれら認証鍵を用いて端末の認証が行われる。認証が終了するとローミング先網はローミング番号を獲得し、ローミング端末及びホーム網に通知する。ローミング端末、ローミング先網、及びホーム網は、それぞれローミング番号と認証鍵とを記憶する。



1

【特許請求の範囲】

【請求項１】　複数の事業者がそれぞれ異なる地域で提供する移動通信サービスを、端末が所属するホーム網以外のローミング先網で受けるためのローミング方式において、前記端末に第１の暗号化鍵を与えるとともに、前記ホーム網に前記暗号化鍵により暗号化された情報を復号する第１の復号鍵を与え、前記端末がローミング先網を介して前記ホーム網へ該端末のＩＤを通知する際に、前記端末において前記ＩＤを前記第１の暗号化鍵を用いて暗号化し、前記ホーム網において前記第１の復号鍵を用いて暗号化されたＩＤを復号するようにしたことを特徴とするローミング方式。

【請求項２】　前記第１の暗号化鍵が公開鍵であり、前記第１の復号鍵が秘密鍵であることを特徴とする請求項１のローミング方式。

【請求項３】　前記ホーム網に第２の暗号化鍵を与えるとともに、前記端末に前記第２の暗号化鍵により暗号化された情報を復号する前記第２の復号鍵を与え、前記ホーム網で生成した認証鍵を前記ローミング先網へ送信するとともに、前記認証鍵を前記第２の暗号化鍵で暗号化して前記ローミング先網を介して前記端末へ送信し、前記端末において前記第２の復号鍵を用いて暗号化された認証鍵を復号するようにしたことを特徴とする請求項１または２のローミング方式。

【請求項４】　前記ローミング先網が乱数を発生し、該乱数を前記暗号化された認証鍵とともに前記端末へ送信し、前記端末において前記乱数と前記第２の復号鍵で復号した認証鍵との演算処理を行って得た演算結果を前記ローミング先網へ返送させ、前記ローミング先網で前記乱数と前記認証鍵との演算処理を行った結果と前記演算結果と比較することにより、認証処理を行うことを特徴とする請求項３のローミング方式。

【請求項５】　前記第２の暗号化鍵が公開鍵であり、前記第２の復号鍵が前記端末に固有の秘密鍵であることを特徴とする請求項３または４のローミング方式。

【請求項６】　前記ホーム網及び前記ローミング先網における前記端末に関するローミング登録を、前記ローミング先網が前記端末に割り当てるローミング番号と前記認証鍵とを用いて行うようにしたことを特徴とする請求項３、４、または、５のローミング方式。

【請求項７】　複数の事業者がそれぞれ異なる地域で提供する移動通信サービスを、端末が所属するホーム網以外のローミング先網で受けることができる移動通信システムにおいて、前記端末が、ローミング時に、自身のＩＤを第１の暗号化鍵で暗号化し、前記ホーム網の網番号とともに、ローミング登録要求信号に含ませて送信する手段と、受信した認証要求信号に含まれる第２の暗号化鍵で暗号化された認証鍵を解読する手段と、受信したローミング受付信号に含まれるローミング番号と前記認証鍵とを関連付けて記憶する記憶手段とを備え、前記前記

2

ローミング先網が、前記ローミング登録要求信号を受信して、前記網番号が示す前記ホーム網へ前記暗号化されたＩＤを含む網間ローミング要求信号を送信する手段と、前記ホーム網からの網間ローミング応答信号に含まれる認証鍵と、前記端末に割り当てるローミング番号とを関連付けて記憶する記憶する手段と、前記網間ローミング応答信号に含まれる第２の暗号化鍵で暗号化された認証鍵を前記認証要求信号として前記端末へ送信する手段と、前記ローミング番号を前記端末及び前記ホーム網へ送信する手段と、前記ホーム網が、前記網間ローミング要求信号を受信し、前記暗号化されたＩＤを解読する手段と、前記認証鍵を生成し、該認証鍵を前記ＩＤに対応する前記第２の暗号化鍵で暗号化し、前記認証鍵と前記暗号化された認証鍵とを含む前記網間ローミング応答信号を送信する手段と、前記ローミング番号を前記ＩＤに関連させて記憶する記憶手段とを有することを特徴とする移動通信システム。

【請求項８】　前記ローミング先網が、前記認証要求信号に含めて送信される乱数を生成する乱数生成手段と、前記乱数と前記認証鍵との演算を行う演算手段と、該演算手段の出力と前記端末からの認証応答信号とを比較する比較手段と、該比較手段の比較結果が一致したとき前記端末にローミング番号を割り当てる手段とを有し、前記端末が、前記乱数と前記復号した認証鍵との演算を行う演算手段と、該演算手段の演算結果を前記認証応答信号として前記ローミング先網へ送信する手段とを有することを特徴とする移動通信システム。

【請求項９】　前記第１の暗号化鍵が前記ホーム網固有の公開鍵であり、前記第２尾暗号化鍵が前記端末固有の公開鍵であることを特徴とする請求項７または８の移動通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ローミング方式に関し、特に、移動通信端末が、契約した事業者以外の事業者のサービスエリアへ移動したときのローミング方式に関する。

【０００２】

【従来の技術】移動通信の分野では、複数の事業者が、それぞれ異なる地域で各々のサービスを提供している。そして、いずれかの事業者と契約した移動通信端末であって、他の事業者の提供するサービスエリアでもにおいて、自端末が契約した事業者のサービスエリア内に位置する場合と同様のサービスが受けられるよう、これら複数の事業者は、ローミングサービスを行っている。

【０００３】図５を参照して、従来の移動端末ローミング方式における、ローミング端末の登録手順を説明する。ローミング端末は、無線基地局からの報知情報を受信しており、その報知情報から、網間ローミングをしたことを知る。つまり、自端末が契約しているホーム網の

サービスエリアを出て、他の事業者（ローミング先網）のサービスエリアに入ったことを知る。そして、ローミング端末は、ローミング先網に対して位置登録要求信号５０１を送信する。この位置登録要求信号５０１には、加入者ＩＤである加入者番号（以下、ＭＳＮ）が含まれている。

【０００４】ローミング先網（の交換局）では、ローミング端末からの位置登録要求信号５０１を受信すると、それに含まれるＭＳＮによって、その端末がローミング端末であると認識する。そして、ローミング先網は、認証処理を行うために、ＭＳＮから知得したホーム網に対して網間認証情報読出要求信号５０２を送信する。この網間認証情報読出要求信号５０２には、ＭＳＮが含まれる。また、ローミング先網は、ローミング端末に対して認証要求信号５０３を送信する。この認証要求信号５０３には、ローミング先網内で生成した認証乱数が含まれる。

【０００５】ホーム網（の交換局）は、自網に所属する端末の認証に必要な認証キーを全て記憶しており、網間認証情報読出要求信号５０２を受信すると、その信号に含まれるＭＳＮが付与された端末の認証キーを検索する。そして、検索した認証キーを網間認証情報読出応答信号５０４でローミング先網へ通知する。

【０００６】また、ローミング端末は、ローミング先網から認証要求信号５０３を受信すると、その認証要求信号５０３に含まれる認証乱数と自信で記憶している固有の認証キーとの演算を、演算回路を用いて行い、その演算結果を認証応答信号５０５でローミング先網に返送する。

【０００７】ローミング先網では、ホーム網からの網間認証情報読出応答信号５０４により得た認証キーと、先にローミング端末へ送信したのと同じ認証乱数との演算処理を行う。そして、ローミング先網は、その演算結果とローミング端末からの認証応答信号５０５に含まれる認証演算結果とを比較する。これらの結果が一致していれば、ローミング端末は、ホーム網に登録されている端末であると判定される。即ち、認証ＯＫとなる。そして、ローミング先網は、そのローミング端末に付与すべきローミング番号（ＲＯＭ）を捕捉し、ＲＯＭを含む位置登録受付信号５０６をローミング端末に送信する。また、ローミング先網は、ＭＳＮ及びＲＯＮを含む網間位置登録要求信号５０７をホーム網へ送信する。

【０００８】ホーム網は、ローミング先網から網間位置登録要求信号５０７を受信すると、その信号に含まれるＭＳＮ及びＲＯＮを記憶する。そして、ＭＳＮに対応する端末に関する情報、例えば、加入者情報、認証キー等を、網間位置登録応答信号５０８により送信する。

【０００９】ローミング先網は、ホーム網から送信されてきた網間位置登録応答信号５０８に含まれる加入者情報及び認証キー等の情報をローミング端末に割り当てたＲＯＮとともに記憶する。

【００１０】上記のようにして、従来のローミング方式では、ローミング端末の登録処理が行われる。これより以後、ローミング端末の位置登録時、発呼時の呼処理は、ローミング先網と、ローミング端末との間で、直接行われる。

【００１１】以上説明したように、従来のローミング処理では、ローミング端末の認証処理を効率良く行うために、初回のローミング登録時に、当該ローミング端末の認証キーをホーム網からローミング先網へ転送している。このため、従来のローミング方式には、認証キーをローミング先網に知られてしまい、漏洩などの危険がある等、セキュリティの面で問題がある。

【００１２】この問題を解決する方法として、特開平４－３５２５２５号公報に開示された方法がある。これは、まず、ローミング端末から位置登録要求を受けたローミング先網が、ローミング処理に使用する仮認定鍵を生成してホーム網に送信しておく。ホーム網は、ローミング先網を経由してローミング端末の認証を行う。ホーム網は、ローミング端末が保持する仮認証鍵設定鍵と同一の鍵を保持しており、認証終了後、この鍵を用いて仮認定鍵を暗号化し、ローミング先網を経由してローミング端末へ送る。ローミング端末は、暗号化された仮認定鍵を、仮認証鍵設定鍵により解読して、仮認証鍵を得る。以降、ローミング先網との認証処理には、この仮認証鍵を使用する。こうして、ローミング先網に、認証鍵を知られることなく、ローミング処理（認証処理）を行うことができる。

【００１３】

【発明が解決しようとする課題】従来のローミング方式では、ローミング端末が位置登録要求を行うには、まず、加入者番号（ＭＳＮ）を、ローミング先網へ送信しなければならない。ローミング端末は、当然、その送信を無線によって行うので、傍受される恐れがあり、ローミング端末の匿名性を確保することができないという問題点がある。

【００１４】本発明は、加入者番号や、認証鍵等の端末固有の情報をローミング先網に通知することなく、ローミング処理を行うことできるローミング方式を提供することを目的とする。

【００１５】また、本発明は、セキュリティの高い移動通信システムを構築することを目的とする。

【００１６】

【課題を解決するための手段】本発明によれば、複数の事業者がそれぞれ異なる地域で提供する移動通信サービスを、端末が所属するホーム網以外のローミング先網で受けるためのローミング方式において、前記端末に第１の暗号化鍵を与えるとともに、前記ホーム網に前記暗号化鍵により暗号化された情報を復号する第１の復号鍵を与え、前記端末がローミング先網を介して前記ホーム網

5

へＩＤを通知する際に、前記端末において前記ＩＤを前記第１の暗号化鍵を用いて暗号化して通知し、前記ホーム網において前記第１の復号鍵を用いて暗号化されたＩＤを復号するようにしたことを特徴とするローミング方式。

【００１７】また、本発明によれば、前記ホーム網に第２の暗号化鍵を与えるとともに、前記端末に前記第２の暗号化鍵により暗号化された情報を復号する前記第２の復号鍵を与え、前記ホーム網で生成した認証鍵を前記ローミング先網へ送信するとともに、前記認証鍵を前記第２の暗号化鍵で暗号化して前記ローミング先網を介して前記端末へ送信し、前記端末において前記第２の復号鍵を用いて暗号化された認証鍵を復号するようにしたことを特徴とするローミング方式が得られる。

【００１８】さらに本発明のよれば、前記ローミング先網が乱数を発生し、該乱数と前記暗号化された認証鍵とを前記端末へ送信し、前記端末において前記乱数と前記第２の復号鍵で復号した認証鍵との演算処理をおこなって演算結果を前記ローミング先網へ返送させ、前記ローミング先網で前記乱数と前記認証鍵との演算処理を行い前記演算結果と比較することにより、認証処理を行うことを特徴とするローミング方式が得られる。

【００１９】さらにまた、本発明によれば、複数の事業者がそれぞれ異なる地域で提供する移動通信サービスを、端末が所属するホーム網以外のローミング先網で受けることができる移動通信システムにおいて、前記端末が、ローミング時に、自身のＩＤを第１の暗号化鍵で暗号化し、前記ホーム網の網番号とともに、ローミング登録要求信号に含ませて送信する手段と、受信した認証要求信号に含まれる第２の暗号化鍵で暗号化された認証鍵を解読する手段と、受信したローミング受付信号に含まれるローミング番号と前記認証鍵とを関連付けて記憶する記憶手段とを備え、前記前記ローミング先網が、前記ローミング登録要求信号を受信して、前記網番号が示す前記ホーム網へ、前記暗号化されたＩＤを含む網間ローミング要求信号を送信する手段と、前記ホーム網からの網間ローミング応答信号に含まれる認証鍵と、前記端末に割り当てるローミング番号とを関連付けて記憶する記憶する手段と、前記網間ローミング応答信号に含まれる第２の暗号化鍵で暗号化された認証鍵を前記認証要求信号として前記端末へ送信する手段と、前記ローミング番号を前記端末及び前記ホーム網へ送信する手段と、前記ホーム網が、前記網間ローミング要求信号を受信し、前記暗号化されたＩＤを解読する手段と、前記認証鍵を生成し、該認証鍵を前記ＩＤに対応する前記第２の暗号化鍵で暗号化し、前記認証鍵と前記暗号化された認証鍵とを含む前記網間ローミング応答信号を送信する手段と、前記ローミング番号を前記ＩＤに関連させて記憶する記憶手段とを有することを特徴とする移動通信システムが得られる。

6

【００２０】

【作用】ローミング端末からのローミング登録要求信号に含まれるＭＳＮは、ホーム網の公開鍵により暗号化されている。このため、ローミング端末のＭＳＮは、ローミング先網を含め第三者に知られることはない。

【００２１】また、ローミング端末とローミング先網との間の認証処理に使用される認証鍵は、ホーム網で生成されるもので、ローミング端末固有のものではない。しかも、ローミング先網からローミング端末への通知は、ローミング端末固有の公開鍵で暗号化された状態で行われるので、ローミング先網以外の第三者に知られることはない。

【００２２】

【発明の実施の形態】以下、図面を参照して、本発明の実施の形態について説明する。まず、図１乃至図３を参照して、本発明のローミング方式を採用する、ローミング端末、ローミング先網、及びホーム網の構成について説明する。

【００２３】図１は、ローミング端末１０のブロック図である。このローミング端末１０は、読み出し専用メモリ（以下、ＲＯＭ）１１ａと書き込み可能なメモリ（以下、ＲＡＭ）１１ｂ、第１の演算部１２ａと第２の演算部１２ｂ、及び無線送受信部１３を有している。また、これらを制御する図示しない制御部を有している。

【００２４】ＲＯＭ１１ａは、その端末に割り当てられた加入者（ＩＤ）番号（以下、ＭＳＮ）と、端末固有の秘密鍵、ホーム網の網番号、及びホーム網の公開鍵等を記憶している。ＲＡＭ１１ｂは、ローミング処理を行う際に、ホーム網から配送される認証鍵を記憶する。また、第１の演算部１２ａは、公開鍵認証方式による演算を行い、第２の演算部１２ｂは、秘密鍵認証方式による演算を行う。

【００２５】図２は、ローミング先網（交換局）２０のブロック図である。このローミング先網２０は、在圏ロケーションレジスタ（以下、ＶＬＲ）２１、演算部２２、無線送受信部２３ａ、通信制御部２３ｂ、呼制御部２４、ＰＮ発振部２５、及び比較部２６を有している。

【００２６】ＶＬＲ２１は、ローミング加入者のローミング番号（以下、ＲＯＮ）、認証鍵、及び位置情報等を格納する。演算部２２は、ローミング端末１０の第１の演算部１２ａと同一のアルゴリズムで、秘密鍵認証方式の演算処理を行う。無線送受信部２３ａは無線基地局（図示せず）とのインタフェース、通信制御部２３ｂは、ローミング端末１０のホーム網を含む他の網とのインタフェースである。また、呼制御部２４は、端末との間のローミング処理、認証処理等の呼制御を行う。ＰＮ発振部２５は、乱数を発生する。比較部２６は、認証結果の判定を行う。

【００２７】図３は、ローミング端末１０のホーム網（交換局）のブロック図である。このホーム網３０は、

ホームロケーションレジスタ（以下、ＨＬＲ）３１ａ、ＲＡＭ３１ｂ、演算部３２、通信制御部３３、呼制御部３４、及び認証鍵生成部３５を有している。

【００２８】ＨＬＲ３１ａは、自網に所属する複数の端末（ローミング端末を含む）のＭＳＮや、各端末の公開鍵等を記憶している。ＲＡＭ３１ｂは、ホーム網３０の秘密鍵を記憶している。演算部３２は、ローミング端末１０の演算部１２ｂと同一のアルゴリズムで、公開鍵認証方式の演算処理を行う。通信制御部３３は、ローミング先網２０を含む他網とのインタフェースである。呼制御部３４は、呼の処理を行う。認証鍵生成部３５は、ローミング端末１０とローミング先網２０との間の認証処理に使用される認証鍵を生成する。

【００２９】以下、これら、ローミング端末１０、ローミング先網２０、及びホーム網３０を含むシステムにおける、ローミング方式について、図４をも参照して説明する。

【００３０】移動通信端末は、移動通信サービスが提供されているエリア内にいるときは、常時移動通信網から送られてくる報知情報により、自端末が存在する位置を認識している。したがって、移動通信端末は、自端末が契約した事業者以外の事業者が提供するサービスエリア内に入ったこと、即ち、ローミング端末１０となったことを認識できる。

【００３１】ローミング端末１０の制御部は、報知情報により自端末が、ローミング先網２０へローミングしたことを認識すると、ＲＯＭ１１ａから、ホーム網の網番号（以下、ＮＷ１）、ＭＳＮ、及びホーム網の公開鍵（以下、Ｋpa）を読み出す。そして、演算部１２ｂに、ＭＳＮとＫpaとを用いた公開鍵認証演算を実行させ、演算結果｛以下、Ｋpa（ＭＳＮ）｝を得る。即ち、演算部１２ｂは、Ｋpaを用いて、ＭＳＮを暗号化し、Ｋpa（ＭＳＮ）を得る。そして、制御部は、無線送受信部１３を介して、ローミング先網２０に対し、ＮＷ１及びＫpa（ＭＳＮ）を含むローミング登録要求信号４０１を送出する。

【００３２】ローミング先網２０では、呼制御部２４が、無線送受信部２３ａを介してローミング登録要求信号４０１を受信する。そして、呼制御部２４は、ローミング登録要求信号４０１に含まれるＮＷ１より、ローミング端末１０のホーム網が、ホーム網３０であることを認識する。そして、呼制御部２４は、受信したローミング登録要求信号４０１に含まれていたＫpa（ＭＳＮ）を含む網間ローミング要求信号４０２を、ホーム網３０へ送出する。

【００３３】ホーム網３０では、呼制御部３４が、通信制御部３３を介して網間ローミング要求信号４０２を受信する。呼制御部３４は、網間ローミング要求信号４０２を受信すると、ＲＡＭ３１ｂからホーム網の秘密鍵（以下、Ｋsa）を読み出し、受信したＫpa（ＭＳＮ）とともに演算部３２へ供給する。演算部３２は、Ｋpa（ＭＳＮ）とＫsaとで公開鍵認証演算処理を行う。つまり、演算部３２は、暗号Ｋpa（ＭＳＮ）をＫsaを用いて解読し、ローミング端末１０のＭＳＮを得る。呼制御部３４は、演算部３２で得たＭＳＮに基づいて、ローミング端末１０の公開鍵Ｋp1を、ＨＬＲ３１ａから取り出す。同時に、呼制御部３４は、認証鍵生成部３５に対して認証鍵の生成を指示する。認証鍵生成部３５は、呼制御部３４からの指示により、任意の方法で、一時的な認証鍵（以下、Ｓａ）を生成して、呼制御部３４へＳａを通知する。

【００３４】続いて、呼制御部３４は、上記のようにして得たＫp1とＳａを演算部３２に通知する。演算部３２は、Ｋp1とＳａとで公開鍵演算処理を行い、演算結果｛以下、Ｋp1（Ｓａ）｝を得る。即ち、演算部３２は、Ｓａを Ｋp1で暗号化する。呼制御部３４は、このＫp1（Ｓａ）と、元のＳａとを含む網間ローミング応答信号４０３を、通信制御部３３を介してローミング先網２０へ返送する。

【００３５】ローミング先網２０では、ホーム網３０から網間ローミング応答信号４０３が返送されてくると、呼制御部２４が、Ｋp1（Ｓａ）とＳａとを取り出す。そして、呼制御部２４は、Ｋp1（Ｓａ）とＰＮ発振部２５で生成した乱数Ｒnとを含む認証要求信号４０４をローミング端末１０に対して送出する。

【００３６】ローミング端末１０では、認証要求信号４０４を受信すると、制御部は、ＲＯＭ１１ａから固有の秘密鍵（以下、Ｋs1）を読み出す。そして、演算部１２ｂに、Ｋp1（Ｓａ）とＫs1との演算処理を実行させる。つまり、演算部１２ｂは、Ｋs1を用いてＫp1（Ｓａ）を解読し、演算結果（以下、Ｓａ'）を得る。さらに制御部は、得られたＳａ'と、先に受信した乱数Ｒnとを用いた演算処理を演算部１２ａに実行させる。換言すると、演算部１２ａは、乱数Ｒnを Ｓａ'で暗号化し、演算結果ＲＥＳ'を得る。制御部は、このＲＥＳ'を認証応答信号４０５として、無線送受信部１３を介してローミング先網２０に送信する。

【００３７】ローミング先網２０では、認証要求信号４０４を送信したあと、演算部２２により、乱数Ｒnと、認証鍵Ｓａとの演算処理が行われ、演算結果ＲＥＳが求められる。この演算結果ＲＥＳは、比較部２６に与えられ、ローミング端末１０から送信されてくる認証応答信号４０５に含まれる演算結果ＲＥＳ'と比較される。比較の結果、これらが一致した場合は、呼制御部２４は、認証ＯＫと判定し、ＶＬＲ２１に、ローミング端末１０に対するＲＯＮの割り当てを指示する。また、不一致の場合、呼制御部２４は、認証ＮＧと判定して、呼接続処理を中止する。

【００３８】ＶＬＲ２１からＲＯＮの通知を受けた呼制御部２４は、無線送信部２３ａを介して、ＲＯＮを含む

ローミング登録受付信号４０６を、ローミング端末１０へ送信する。また、呼制御部２４は、ＲＯＮとＳａ とを含む網間ローミング登録要求信号４０７を、通信制御部２３ｂを介してホーム網３０へ送信する。

【００３９】ローミング端末１０では、ローミング登録受付信号４０６を受信すると、制御部が、受信した信号に含まれるＲＯＮと、先の演算で求めたＳａ'とをＲＡＭ１１ｂに格納する。

【００４０】ホーム網３０では、網間ローミング登録要求信号４０７を受信すると、呼制御部３４が、この信号に含まれるＳａ とＲＯＮとを、先のＭＳＮに関連付けてＨＬＲ２１に格納する。そして、呼制御部３４は、登録を受け付けたことを示す網間ローミング登録受付信号４０８を、ローミング先網２０へ送信する。

【００４１】ローミング先網２０の呼制御部２４は、網間登録受付信号４０８を受信すると、ＲＯＮとＳａ とをＶＬＲ２１に格納する。

【００４２】以上のようにして、ローミング端末の登録処理（ローミング処理）は完了する。このあと、ローミング端末１０からの発信時、及び、ローミング端末１０への着信時における接続処理は、以下のように行われる。

【００４３】ローミング端末１０から発信（発呼）を行う場合、ローミング端末１０は、ＲＯＮを含む発信要求信号を、ローミング先網２０へ送出する。

【００４４】ローミング先網２０は、端末からの発信要求信号を受信すると、この信号に含まれるＲＯＮにより、発呼を要求している端末が、ローミング端末であることを認識する。そして、ローミング先網２０は、ＶＬＲ２１より、ＲＯＮに対応する端末の認証鍵Ｓａ を取り出し、この認証鍵Ｓａ を用いて認証処理を行う。そして、認証処理が正常に終了した後、呼接続処理に移行する。

【００４５】また、ローミング端末１０への着信があった場合、ホーム網３０は、ＨＬＲ３１ａに格納されているＲＯＮから、該当する端末がローミング中であることを認識する。そして、ホーム網３０は、ローミング先網２０へ着呼を通知する。この通知に使用される通知信号の着信アドレスには、ＲＯＮが設定される。

【００４６】ローミング先網２０は、ホーム網３０からの通知信号に基づいて、ＶＬＲ２１から、ＲＯＮに対応する端末の位置情報、認証鍵Ｓａ 等の情報を取り出し、着信接続処理を行う。

【００４７】

【発明の効果】本発明のよれば、ローミング端末から、ローミング先網を介してホーム網へ送信されるＭＳＮをホーム網の公開鍵で暗号化して送信するようにしたことで、無線区間で傍受されてもＭＳＮが露呈することがない。しかも、ローミング先網に対しても秘密にすることができる。

【００４８】また、ホーム網からローミング先網へ送信される認証鍵は、端末に固有のものではなく、ホーム網で一時的に生成したものなので、ローミング先網で認証鍵が漏洩したとしても、セキュリティ上の大きな問題とはならない。

【図面の簡単な説明】

【図１】本発明のローミング方式が適用されるローミング端末のブロック図である。

【図２】本発明のローミング方式が適用されるローミング先網のブロック図である。

【図３】本発明のローミング方式が適用されるホーム網のブロック図である。

【図４】本発明のローミング方式の一実施の形態を示す図である。

【図５】従来のローミング方式のローミング端末登録処理の手順を説明するための図である。

【符号の説明】

１０	ローミング端末
１１ａ	読み出し専用メモリ（ＲＯＭ）
１１ｂ	書き込み可能なメモリ（ＲＡＭ）
１２ａ	第１の演算部
１２ｂ	第２の演算部
１３	無線送受信部
２０	ローミング先網
２１	在圏ロケーションレジスタ（ＶＬＲ）
２２	演算部
２３ａ	無線送受信部
２３ｂ	通信制御部
２４	呼制御部
２５	ＰＮ発振部
２６	比較部
３０	ホーム網
３１ａ	ホームロケーションレジスタ（ＨＬＲ）
３１ｂ	ＲＡＭ
３２	演算部
３３	通信制御部
３４	呼制御部
３５	認証鍵生成部
４０１	ローミング登録要求信号
４０２	網間ローミング要求信号
４０３	網間ローミング応答信号
４０４	認証要求信号
４０５	認証応答信号
４０６	ローミング登録受付信号
４０７	網間ローミング登録要求信号
４０８	網間ローミング登録受付信号
５０１	位置登録要求信号
５０２	網間認証情報読出要求信号
５０３	認証要求信号
５０４	網間認証情報読出応答信号

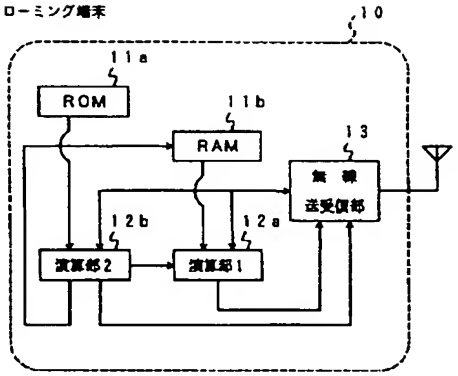
11

505　認証応答信号
506　位置登録受付信号

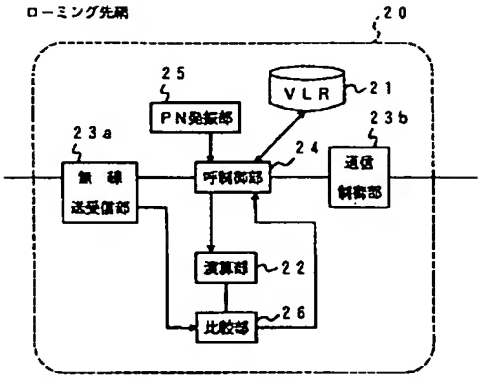
12

507　網間位置登録要求信号
508　網間位置登録応答信号

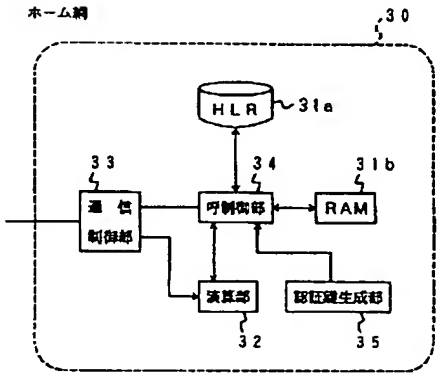
【図1】



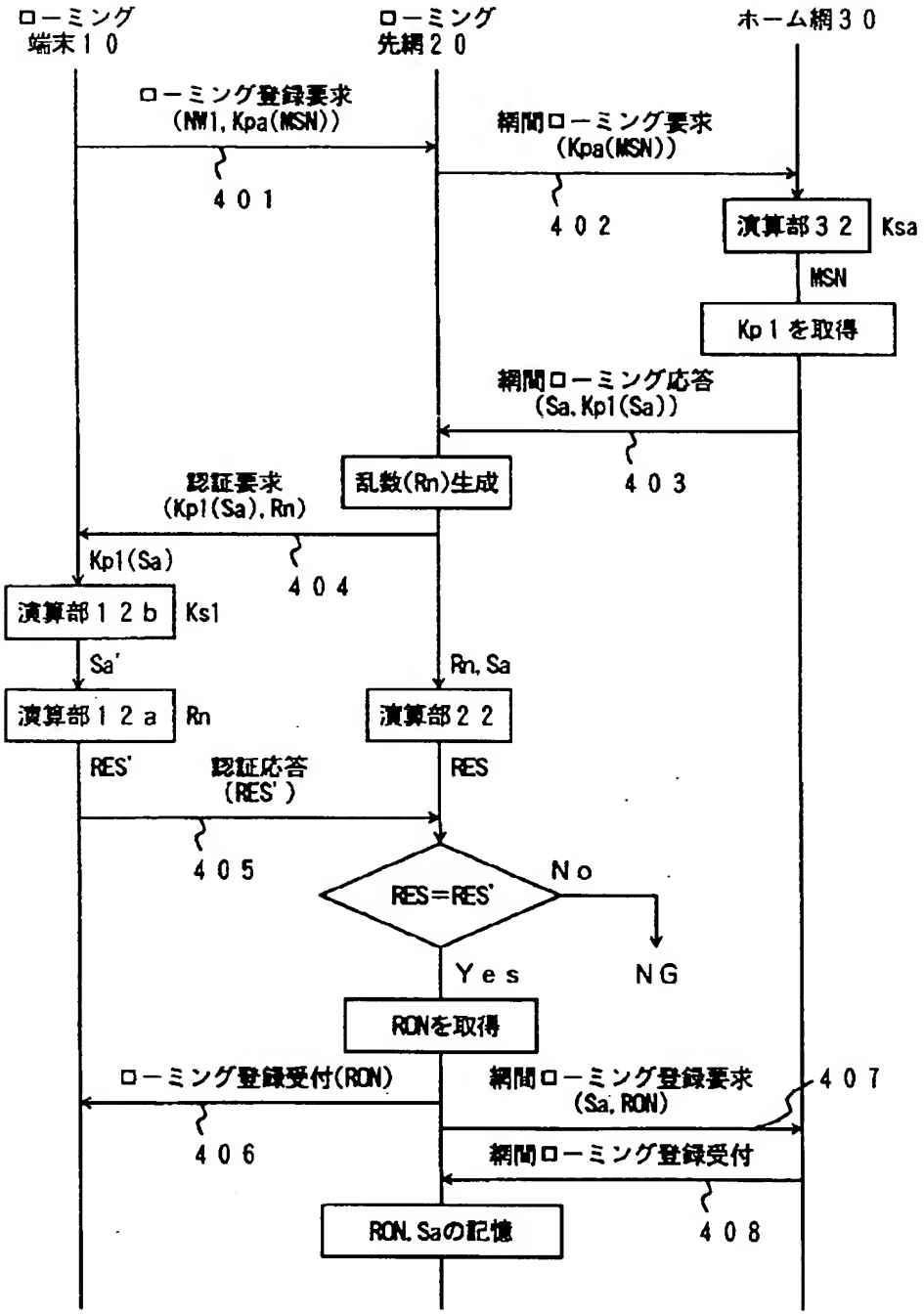
【図2】



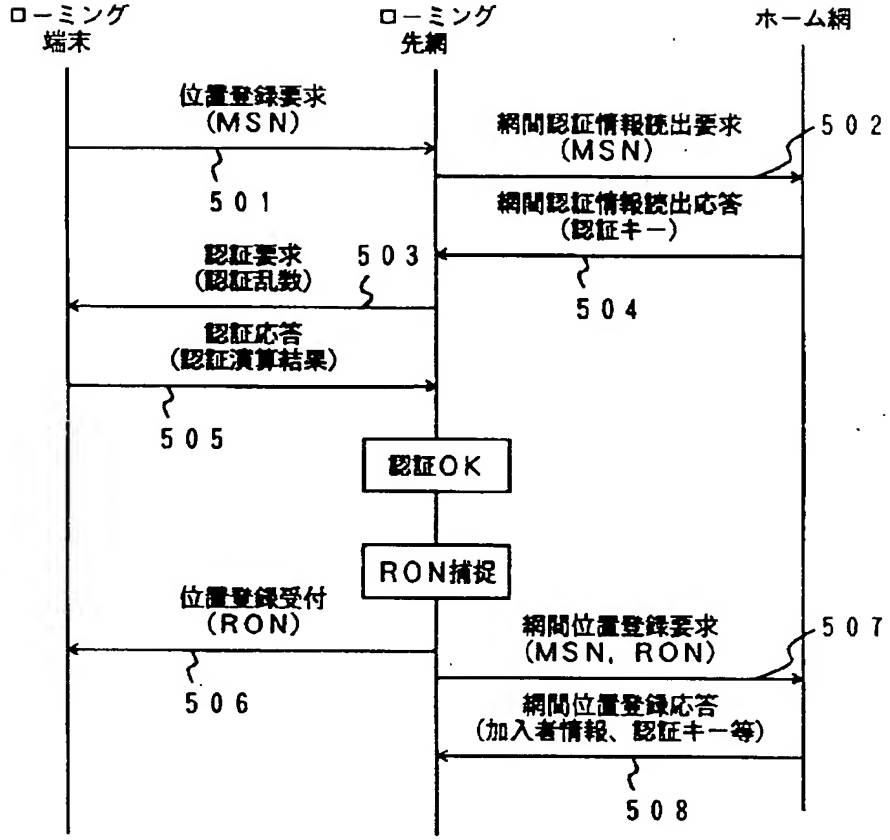
【図3】



【図4】


ローミング
端末10
ローミング
先網20
ホーム網30
ローミング登録要求
(NW1, Kpa(MSN))
401
網間ローミング要求
(Kpa(MSN))
402
演算部32
Ksa
MSN
Kp1を取得
網間ローミング応答
(Sa, Kp1(Sa))
403
乱数(Rn)生成
認証要求
(Kp1(Sa), Rn)
404
Kp1(Sa)
演算部12b
Ks1
Sa'
Rn, Sa
演算部12a
Rn
演算部22
RES'
認証応答
(RES')
RES
405
RES=RES'
No
Yes
NG
RONを取得
ローミング登録受付(RON)
406
網間ローミング登録要求
(Sa, RON)
407
網間ローミング登録受付
408
RON, Saの記憶

【図5】


ローミング
端末
ローミング
先網
ホーム網
位置登録要求
(MSN)
501
網間認証情報読出要求
(MSN)
502
網間認証情報読出応答
(認証キー)
504
認証要求
(認証乱数)
503
認証応答
(認証演算結果)
505
認証OK
RON捕捉
位置登録受付
(RON)
506
網間位置登録要求
(MSN, RON)
507
網間位置登録応答
(加入者情報、認証キー等)
508